DECLARATION

I, Alexa Morris, based on my personal knowledge and information, hereby declare as follows:

1. I am Managing Director of the IETF Administration LLC and have held that position since the LLC was formed in August 2018. Prior to that, starting on January 1, 2008, I was the Executive Director of the Internet Engineering Task Force, which was an activity of the Internet Society. Since the business of IETF did not change in any materially relevant manner with the formation of the LLC, I will collectively refer to both the activity and the LLC as IETF.

2. One of my responsibilities with IETF has been to act as the custodian of Internet-Drafts and records relating to Internet-Drafts. I am familiar with the record keeping practices relating to Internet-Drafts, including the creation and maintenance of such records.

3. I hereby declare that all statements made herein are of my own knowledge and information contained in the business records of IETF and are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements may be punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

4. If depositions regarding the information in this declaration are required, the deposition should be taken by phone or videoconference or, if it must be in person, should be in California.

5. Since 1998, it has been the regular practice of the IETF to publish Internet-Drafts and make them available to the public on its website at www.ietf.org (the IETF website). The IETF maintains copies of Internet-Drafts in the ordinary course of its regularly conducted activities.

6. Any Internet-Draft published on the IETF website was reasonably accessible to the public and was disseminated or otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence could have located it. In particular, the Internet-Drafts were indexed and searchable on the IETF website.

7. Internet-Drafts are posted to an IETF online directory. When an Internet-Draft is published, an announcement of its publication that describes the Internet-Draft is disseminated. Typically, that dated announcement is made within 24 hours of the publication of the Internet-Draft. The announcement is kept in the IETF email archive and the date is affixed automatically.

8. The records of posting the Internet-Drafts in the IETF online repository are kept in the course of the IETF's regularly conducted activity and ordinary course of business. The records are made pursuant to established procedures and are relied upon by the IETF in the performance of its functions.

9. It is the regular practice of the IETF to make and keep the records in the online repository.

10. Exhibit 1 is a true and correct copy of an announcement of the publication of draft-calhoun-seamoby-lwapp-03, titled "Light Weight Access Point Protocol (LWAPP)." I have determined that an announcement of the publication of this Internet-Draft was made on July 3, 2003. Therefore, based on the normal practice of the IETF, that Internet-Draft was reasonably available to the public within 24 hours of that announcement. At that time, the Internet-Draft would have been disseminated or otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, could have located it.

11. Exhibit 2 is a true and correct copy of an announcement of the publication of draft-mani-capwap-arch-00, titled "Architecture for Control and Provisioning of Wireless Access Points (CAPWAP)." I have determined that an announcement of the publication of this Internet-Draft was made on October 22, 2003. Therefore, based on the normal practice of the IETF, that Internet-Draft was reasonably available to the public within 24 hours of that announcement. At that time, the Internet-Draft would have been disseminated or otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, could have located it.

Pursuant to Section 1746 of Title 28 of United States Code, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that the foregoing is based upon personal knowledge and information and is believed to be true.

Date: July 31, 2023

By: ______________________
Alexa Morris

4866-4349-3491

Network Working Group P. Calhoun
Internet-Draft B. O'Hara
Expires: December 27, 2003 S. Kelly
R. Suri
Airespace
D. Funato
DoCoMo USA Labs
M. Vakulenko
Legra Systems, Inc.
June 28, 2003

Light Weight Access Point Protocol (LWAPP)
draft-calhoun-seamoby-lwapp-03

Status of this Memo

Copyright Notice

Abstract

While conventional wisdom has it that wireless Access Points are strictly Layer 2 bridges, such devices today perform some higher functions that are performed by routers or switches in wired networks in addition to bridging between wired and wireless networks. For example, in 802.11 networks, Access Points can function as Network

Access Servers. For this reason, Access Points have IP addresses and can function as IP devices.

This document describes the Light Weight Access Point Protocol which is a protocol allowing a router or switch to interoperably control

and manage a collection of wireless Access Points. The protocol is independent of wireleess Layer 2 technology, but an 802.11 binding is provided.

Table of Contents

1. Introduction

Current wireless Access Points (AP) perform functions that require IP level service, and so they are not strictly Layer 2 devices, conventional wisdom to the contrary notwithstanding. However, unlike wired network elements, Access Points require an additional set of management and control functions related to their primary function of bridging between the wireless and wired medium. The details of how these functions are implemented are naturally dependent on the particular Layer 2 wireless protocol, but in many cases the overall control and management functions themselves are generic and could apply to any wireless Layer 2 protocol. Today, protocols for managing access points are either Layer 2 specific or non-existent (if the Access Points are self-contained). The emergence of simple Access Points in 802.11 that are managed by a router or switch (also known as an Access router, or AR) suggests that having a standardized, interoperable protocol could radically simplify the deployment and management of wireless networks, a trend that could become more important in new wireless Layer 2 protocols. Such a protocol could also better support interoperability between Layer 2 devices supporting different wireless Layer 2 technologies, allowing smoother intertechnology handovers.

LWAPP assumes a network configuration that consists of multiple APs connected either via layer 2 (Ethernet), or layer 3 (IP) to an AR. The APs can be considered as remote RF interfaces, being controlled by the AR (see Figure 1). The AP forwards all 802.11 frames received to the AR via the LWAPP protocol, which processes the frames. Similarly, packets from authorized mobiles are forwarded by the AP to the AR via this protocol.

```
+-+          802.11frames        +-+
| |--------------------------------| |
| |                +-+             | |
| |--------------| |---------------| |
| |  802.11 PHY/ | |     LWAPP     | |
| | MAC sublayer | |               | |
+-+              +-+               +-+
STA              AP                AR
```

Figure 1: LWAPP Architecture

Security is another aspect of Access Point management that is not well served by existing solutions. Provisioning Access Points with security credentials, and managing which Access Points are authorized to provide service are today handled by proprietary solutions. Allowing these functions to be performed from a centralized router or switch in an interoperable fashion increases managability and allows network operators to more tightly control their wireless network infrastructure. Further, since the interface between the AP and the AR is point-to-point, it is now possible to centralize user or station (STA) authentication (such as 802.1x, see Figure 2) as well as policy enforcement functions, without the risk of 802.11 leakage into the network.

```
        +-+          EAPOL frames          +-+  EAP/RADIUS  +-+
        | |--------------------------------| |--------------| |
        | |             +-+                | |              | |
        | |-------------| |----------------| |--------------| |
        | |  802.11 PHY/ | |     LWAPP      | |              | |
        | | MAC sublayer | |                | |              | |
        +-+             +-+                +-+              +-+
        STA             AP                 AR               AAA
```

Figure 2: 802.1X Authentication in the AR

This document describes the Light Weight Access Point Protocol (LWAPP), an inter-operable IP protocol allowing an AR to manage a collection of APs. The protocol is defined to be independent of Layer 2 technology, but an 802.11 binding is provided for use in growing 802.11 wireless LAN networks.

Goals

The following are goals for this protocol:

1. Reduction of the amount of protocol code being executed at the light weight AP, to apply the computing resource of the AP to the application of wireless access, rather than bridge forwarding and filtering. This makes the most efficient use of the computing power available in APs that are the subject of severe cost pressure.

2. Centralization of the bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN, to apply the capabilities of network processing silicon to the WLAN, as it

has already been applied to wired LANs.

3. Providing a generic encapsulation and transport mechanism, the

protocol may be applied to other access protocols in the future.

The LWAPP protocol concerns itself solely on the interface between the AP and the AR. Inter-AR, or mobile to AR communication is strictly outside the scope of this document.

1.1 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [8].

2. Protocol Overview

LWAPP is a generic protocol defining how Light-Weight Access Points communicate with Access Routers. Access Points and Access Routers may be connected either by means of Layer 2 network or by means of a routed IP network.

LWAPP messages and procedures defined in this document apply for both transports unless specified otherwise. the transport independence is achieved via the LWAPP Transport Layer (LTL), which is defined in section Section 7. LTL defines the framing, fragmentation/ reassembly, and multiplexing services to LWAPP for each transport.

The Light Weight Access Protocol (LWAPP) begins with a discovery phase, whereby the APs send a Discovery Request frame, causing any Access Router (AR) [9], receiving that frame to respond with a Discovery Reply. From the Discovery Replies received, an Access Point (AP) will select an AR with which to associate, using the Join Request and Join Reply. The Join Request also provides an MTU discovery mechanism, to determine whether there is support for the transport of jumbo frames between the AP and it's AR. If support for jumbo frames is not present, the LWAPP frames will be fragmented to the maximum length discovered to be supported by the layer 2 network.

Once the AP and the AR have joined, a configuration exchange is accomplished that will upgrade the version of the code running on the AP to match that of the AR, if necessary, and will provision the APs. The provisioning of APs includes the typical name (802.11 Service Set Identifier, SSID), and security parameters, the data rates to be advertised as well as the radio channel (channels, if the AP is capable of operating more than one 802.11 MAC and PHY simultaneously) to be used. Finally, the APs are enabled for operation.

When the AP and AR have one or more WLANs provisioned and enabled, the LWAPP encapsulates the 802.11 Data and Management frames, to transport them between the AP and AR. LWAPP will fragment its packets, if the size of the encapsulated 802.11 Data or Management frames causes the resultant LWAPP packet to exceed the MTU supported between the AP and AR. Fragmented LWAPP packets are reassembled to reconstitute the original encapsulated payload.

In addition to the functions thus far described, LWAPP also provides for the delivery of commands from the AR to the AP for the management of 802.11 devices that are communicating with the AP. This may include the creation of local data structures in the AP for the 802.11 devices and the collection of statistical information about the communication between the AP and the 802.11 devices. LWAPP provides the ability for the AR to obtain any statistical information

collected by the AP.

3. Definitions

This Document uses terminology defined in [9]

4. LWAPP Packet Format

This section contains the general packet header format. The LWAPP protocol is designed to be transport agnostic. Transport details can be found in the section entitled Section 7.

4.1 LWAPP Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|VER| RID |       Reserved        |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Ctl/Stat             |   Payload...  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.1.1 Flags Field

The first byte contains several flag fields.

4.1.2 VER field

The VER field identifies the LWAPP protocol version carried in this packet. For this version of the protocol, the value of this field is 0.

4.1.3 RID

The RID field contains the Radio Identifier. For APs that contain more than one radio, this field is used to idenfity each Radio.

4.1.4 Reserved

The reserved field MUST be set to zero unless these bits are defined for use with a specific transport (see Section 7.1).

4.1.5 Length

The value of this field is unsigned and indicates the number of bytes in the Payload field.

4.1.6 Control/Status

The interpretation of this field depends on the direction of transmission of the packet.

4.1.6.1 Status

When an LWAPP packet is transmitted from an AP to a AR, this field indicates link layer information associated with the frame. When the C bit is 0, this field is transmitted as zero and ignored on reception.

For 802.11, the signal strength and signal to noise ratio with which an 802.11 frame was received, encoded in the following manner:

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     RSSI      |     SNR       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.1.6.1.1 RSSI

RSSI is a signed, 8-bit value. It is the received signal strength indication, in dBm.

4.1.6.1.2 SNR

SNR is a signed, 8-bit value. It is the signal to noise ratio of the received 802.11 frame, in dB.

4.1.6.2 Control

When an LWAPP packet is transmitted from an AR to an AP, this field indicates on which WLANs the encapsulated 802.11 frame is to be transmitted. For unicast packets, this field is not used by the AP, but for broadcast or multicast packets, the AP may require this information if it provides encryption services.

Given that a single broadcast or multicast packet may need to be sent to multiple wireless LANs (presumably each with a different broadcast key), this field must be a bit field. The bit position indicates the WLAN ID (see Section 5.27) the frame is to be transmitted to.

The Control field is encoded in the following manner:

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          WLAN ID(s)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.1.7 Payload

The Payload field contains data equal in size to the value of the Length field, found within the LWAPP header.

4.2 LWAPP Control Messages

The LWAPP Control protocol provides a communication channel between the AP and the AR and falls into the following distinct messages types:

Control Channel Management: Messages that fall within this classification are used for the discovery of ARs by the APs as well as the establishment and maintenance of an LWAPP control channel.

AR Configuration: The AR Configuration messages are used by the AR to push a specific configuration to the APs it has a control channel with. Messages that deal with the retrieval of statistics from the AP also fall in this category.

Mobile Session Management: Mobile session management messages are used by the AR to push specific mobile policies to the AP.

Firmware Management: Messages in this category are used by the AR to push a new firmware image down to the AP.

4.2.1 LWAPP State Machine

The LWAPP Control Messages are used to communicate between the AR and the AP. The following state diagram represents the lifecycle of an AP-AR session:


```
   ---------------------------------------------------------------------
```

```
                   +------+(--------------------------------\
                   | Idle |                                  |
                   +------+                                  |
                      /         +---------+--)+------------+ |
                     /          |   Run   |    | Key Update | |
                    v           +---------+(--+------------+ |
           +-----------+          ^   |   |                  |
           | Discovery |          |   v   \----------->+-------+
           +-----------+         +-----------+        | Reset |
             | ^    \        /--)| Configure |        +-------+
             v |     \      /    +-----------+            ^
      +---------+     v    /                              |
      | Sulking |   +------+            +------------+    |
      +---------+   | Join |------------)| Image Data |--/
                    +------+            +------------+

                  Figure 3: LWAPP State Machine

   ---------------------------------------------------------------------
```

Each of the states above correspond to an LWAPP control message type,defined later in this document.

4.2.2 Control Message Format

All LWAPP control messages are sent encapsulated within the LWAPP header (see Section 4.1) with the following header values:

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Msg Type   |    Seq Num    |      Msg Element Length       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                           Session ID                          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Msg Element [0..N]        |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.2.2.1 Message Type

The Message Type field identifies the function of the LWAPP control message. The valid values for Message Type are the following:

Description	Value

Description	Value
Discovery Request	1
Discovery Reply	2
Join Request	3
Join Reply	4
Configure Request	5
Configure Response	6
Configuration Update Request	7
Configuration Update Response	8
Statistics Report	9
Statistics Report Response	10

```
          Reserved                         11-16
          Echo Request                        17
          Echo Response                       18
          Image Data Request                  19
          Image Data Response                 20
          Reset Request                       21
          Reset Response                      22
          Key Update Request                  23
          Key Update Response                 24
          Reserved                         25-26
          Key Update Trigger                  27
```

4.2.2.2 Sequence Number

The Sequence Number Field is an identifier value to match request/ response packet exchanges. When an LWAPP packet with a request message type is received, the value of the sequence number field is copied into the corresponding response packet.

4.2.2.3 Msg Element Length

The Length field indicates the number of bytes following the Session ID field.

4.2.2.4 Session ID

The Session ID is a 32-bit unsigned integer that is used to identify the security context for encrypted exchanges between the AP and the AR.

4.2.2.5 Message Element[0..N]

The message element(s) carry the information pertinent to each of the control message types. The total length of the message elements is indicated in the Msg Element Length field.

The format of a message element uses the standard TLV format shown here:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      Type     |             Length            |   Value ...   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where Type identifies the character of the information carried in the Value field and Length indicates the number of bytes in the Value field.

The LWAPP message elements are defined in Section 5

4.2.3 Control Channel Management

The Control Channel Management messages are used by the AP and AR to create and maintain a channel of communication on which various other commands may be transmitted, such as configuration, firmware update, etc.

4.2.3.1 Discovery Requests

The Discovery Request is used by the AP to automatically discovery potential ARs available in the network. An AP must transmit this command even if it has a statically configured AR, as it is a required step in the LWAPP state machine.

4.2.3.1.1 Sending Discovery Requests

Discovery Requests MUST be sent by an AP in the Discover state after waiting for a random delay less than MaxDiscoveryInterval, after an AP first comes up or is (re)initialized. An AP MUST send no more than a maximum of MaxDiscoveries discoveries, waiting for a random delay less than MaxDiscoveryInterval between each successive discovery.

This is to prevent an explosion of AP Discoveries. An example of this occurring would be when many APs are powered on at the same time.

Discovery requests MUST be sent by an AP when no echo responses are received for NeighborDeadInterval and the AP returns to the discover state. Discovery requests are sent after NeighborDeadInterval, they MUST be sent after waiting for a random delay less than MaxDiscoveryInterval. An AP MAY send up to a maximum of MaxDiscoveries discoveries, waiting for a random delay less than

MaxDiscoveryInterval between each successive discovery.

If a discovery response is not received after sending the maximum number of discovery requests, the AP enters the Sulking state and MUST wait for an interval equal to SilentInterval before sending further discovery requests.

The Discovery Request message may be sent as a unicast, broadcast or multicast message.

TODO: Specify exponential backoff of discovery requests.

4.2.3.1.2 Format of a Discovery Request

The Discovery Request carries the following message elements:

    AP Payload
    Radio Payload (one for each radio in the AP)

4.2.3.1.3 Receiving Discovery Requests

Upon receiving a discovery request, the AR will respond with a Discovery Reply sent to the address in the source address of the received discovery request.

4.2.3.2 Discovery Reply

The Discovery Reply is a mechanism by which an AR advertises its services to requesting APs.

4.2.3.2.1 Sending Discovery Replies

Discovery Replies are sent by an AR after receiving a Discovery Request.

4.2.3.2.2 Format of a Discovery Reply

The Discovery Reply carries the following message elements:

AR Payload
AR Name Payload

4.2.3.2.3 Receiving Discovery Replies

When an AP receives a Discovery Reply, it MUST wait for an interval not less than DiscoveryInterval for receipt of additional discovery

replies. After the DiscoveryInterval elapses, the AP enters the Joining state and will select one of the ARs that sent a discovery reply and send a Join Request to that AR.

4.2.3.3 Join Request

The Join Request is used by an AP to inform an AR that it wishes to provide services through it.

4.2.3.3.1 Sending Join Requests

Join Requests are sent by an AP in the Joining state after receiving one or more Discovery Replies. The Join Request is also used as an MTU discovery mechanism by the AP. The AP issues a Join Request with a Test message element, bringing the total size of the message to exceed MTU.

The initial Join Request is padded with the Test message element to 1596 bytes. If a Join Reply is received, the AP can forward frames without requiring any fragmentation. If no Join Reply is received, it issues a second Join Request padded with the Test Payload to a total of 1500 bytes. The AP continues to cycle from large (1596) to small (1500) packets until a Join Reply has been received, or until both packets sizes have been retransmitted 3 times. If the Join Reply is not received after the maximum number of retransmissions, the AP MUST abandon the AR and restart the discovery phase.

4.2.3.3.2 Format of a Join Request

The Join Request carries the following message elements:

AR Address Payload
AP Payload
AP Name Payload
Location Data
Radio Payload (one for each radio)
Certificate

Session ID
Test

4.2.3.3.3 Receiving Join Requests

When an AR receives a Join Request it will respond with a Join Reply. The AR validates the certificate found in the request. If valid, the AR generates a session key which will be used to secure the control frames it exchanges with the AP. When the AR issues the Join Reply, the AR creates a context for the session with the AP.

Details on the key generation is found in appendix A.

4.2.3.4 Join Reply

The Join Reply is sent by the AR to indicate to an AP whether it is capable and willing to provide service to it.

4.2.3.4.1 Sending Join Replies

Join Replies are sent by the AR after receiving a Join Request. Once the Join Reply has been sent, the heartbeat timer is initiated for the session. Expiration of the timer will result in delete of the AR-AP session. The timer is refreshed upon receipt of the Echo Request.

4.2.3.4.2 Format of a Join Reply

The Join Reply carries the following message elements:

Result Code
Certificate
Session Key

4.2.3.4.3 Receiving Join Replies

When an AP receives a Join Reply it enters the Joined state and initiates the Configure Request to the AR to which it is now joined. Upon entering the Joined state, the AP begins timing an interval equal to NeighborDeadInterval. Expiration of the timer will result in the transmission of the Echo Request.

4.2.3.5 Echo Request

The Echo Request message is a keepalive mechanism for the LWAPP control message.

4.2.3.5.1 Sending Echo Requests

Echo Requests are sent by an AP in the Join or Run state to determine the state of the connection between the AP and the AR.

4.2.3.5.2 Format of a Echo Request

The Echo Request carries no message elements.

4.2.3.5.3 Receiving Echo Requests

When an AR receives an Echo Request it responds with a Echo Response.

4.2.3.6 Echo Response

The Echo Response acknowledges the Echo Request.

4.2.3.6.1 Sending Echo Responses

Echo Responses are sent by an AR after receiving an Echo Request.

4.2.3.6.2 Format of a Echo Response

The Echo Response carries no message elements.

4.2.3.6.3 Receiving Echo Responses

When an AP receives an Echo Response it resets the timer that is timing the NeighborDeadInterval. If the NeighborDeadInterval timer expires prior to receiving an Echo Response, the AP enters the Discovery state.

4.2.3.7 Key Update Request

The Key Update Request updates the LWAPP session key used to secure messages between the AP and the AR.

4.2.3.7.1 Sending Key Update Requests

Key Update Requests are sent by an AP in the Run state to update a session key. The Session ID message element MUST include a new session identifier.

4.2.3.7.2 Format of a Key Update Request

The Key Update Request carries the following message elements:

Session ID

4.2.3.7.3 Receiving Key Update Requests

When a AR receives a Key Update Request it generates a new key (see appendix A) and responds with a Key Update Response.

4.2.3.8 Key Update Response

The Key Update Response updates the LWAPP session key used to secure messages between the AP and the AR, and acknowledges the Key Update Request.

4.2.3.8.1 Sending Key Update Responses

Key Update Responses are sent by a AR after receiving a Key Update Request. The Key Update Responses is secured using public key cryptography.

4.2.3.8.2 Format of a Key Update Response

The Key Update Response carries the following message elements:

Session Key

4.2.3.8.3 Receiving Key Update Responses

When an AP receives a Key Update Response it will use the information contained in the Session Key message element to determine the keying material used to encrypt the LWAPP communications between the AP and the AR.

4.2.3.9 Key Update Trigger

The Key Update Trigger is used by the AR to request that a Key Update Request be initiated by the AP.

4.2.3.9.1 Sending Key Update Trigger

Key Update Requests are sent by an AR in the Run state to inform the AP to initiate a Key Update Request message.

4.2.3.9.2 Format of a Key Update Trigger

The Key Update Request carries the following message elements:

Session ID

4.2.3.9.3 Receiving Key Update Trigger

When a AP receives a Key Update Trigger it generates a key Update Request.

4.2.4 AR Configuration

The AR Configuration messages are used by the LWAPP peers to exchange and push configuration as well as for the AR to retrieve statistics from the AP.

4.2.4.1 Configure Request

The Configure Request message is sent by an AP to send its current configuration to its AR.

4.2.4.1.1 Sending Configure Requests

Configure Requests are sent by an AP after receiving a Join Reply.

4.2.4.1.2 Format of a Configure Request

The Configure Request carries the following message elements:

```
Administrative State (for the AP)
AR Name
Administrative State (for each radio)
AP WLAN Radio Configuration (for each radio)
Multi-domain Capability (for each radio)
MAC Operation (for each radio)
PHY TX Power (for each radio)
PHY TX Power Level (for each Radio)
PHY DSSS Payload or PHY OFDM Payload (for each radio)
Antenna (for each radio)
Supported Rates (for each radio)
```

4.2.4.1.3 Receiving Configure Requests

When an AR receives a Configure Request it will act upon the content of the packet and respond to the AP with a Configure Response.

4.2.4.2 Configure Response

The Configure Response message is sent by an AR and provides an opportunity for the AR to override an AP's configuration.

4.2.4.2.1 Sending Configure Responses

Configure Responses are sent by an AR after receiving a Configure Request.

4.2.4.2.2 Format of a Configure Response

The Configure Response carries the following message elements:

```
 Result Code
AP WLAN Radio Configuration (for each radio)
Operational Rate Set (for each radio)
Multi-domain Capability (for each radio)
MAC Operation (for each radio)
PHY Tx Power (for each Radio)
PHY DSSS or PHY OFDM Payload (for each radio)
Antenna (for each radio)
```

4.2.4.2.3 Receiving Configure Responses

When an AP receives a Configure Response it acts upon the content of the packet, as appropriate.

4.2.4.3 Configuration Update Request

The Configuration Update Request is a message initiated by the AR to update the configuration of an AP while in the Run state.

4.2.4.3.1 Sending Configuration Update Requests

Configure Update Requests are sent by the AR to provision the AP while in the Run state. This is used to modify the configuration of the AP while it is operational.

4.2.4.3.2 Format of a Configure Update Request

The Configure Command Request carries any message elements, except the following:

```
    Result Code                    1
    AR Address                     2
    AP Payload                     3
    AR Payload                     5
    AP WLAN Radio Configuration    7
    Reserved                      16
     Test                          17
    Reserved                   18-24
    AR Name                       30
    Image Download                31
    Image Data                    32
    Statistics                    37
    Reserved                   38-42
```



```
    Certificate                   43
    Session Key                   45
    Reserved                   46-49
```

4.2.4.3.3 Receiving Configuration Update Requests

When an AR receives a Configuration Update Request it will respond with a Configuration Update Reply, with the appropriate Result Code.

4.2.4.4 Configuration Update Response

The Configuration Update Response is the acknowledgement message for the Configuration Update Request.

4.2.4.4.1 Sending Configuration Update Responses

Configuration Update Responses are sent by an AP after receiving a Configuration Update Request.

4.2.4.4.2 Format of a Configuration Update Response

The Configuration Update Response carries the following message elements:

```
     Result Code                   1
```

4.2.4.4.3 Receiving Configure Update Responses

When an AR receives a Configure Update Response it knows that the configuration was accepted (or not) by the AP.

4.2.4.5 Statistics Report

Statistics Reports are used for statistics collection at the AR.

4.2.4.5.1 Sending Statistics Reports

Statistics Reports are sent by an AP periodically, based on the configuration, to transfer statistics to the AR.

4.2.4.5.2 Format of a Statistics Report

The Statistics Report carries the following message elements:

Statistics

4.2.4.5.3 Receiving Statistics Report

When an AR receives a Statistics Report it will respond with a Statistics Response.

4.2.4.6 Statistics Response

Statistics Response acknowledges the Statistics Report.

4.2.4.6.1 Sending Statistics Responses

Statistics Responses are sent by an AR after receiving a Statistics Report.

4.2.4.6.2 Format of a Statistics Response

The Statistics Response carries no message elements.

4.2.4.6.3 Receiving Statistics Responses

The Statistics Response is simply an acknowledgement of the Statistics Report.

4.2.4.7 Reset Request

The Reset Request is used to cause an AP to reboot.

4.2.4.7.1 Sending Reset Requests

Reset Requests are sent by an AR to cause an AP to reinitialize its operation.

4.2.4.7.2 Format of a Reset Request

The Reset Request carries no message elements.

4.2.4.7.3 Receiving Reset Requests

When an AP receives a Reset Request it will respond with a Reset Response and then reinitialize itself.

4.2.4.8 Reset Response

The Reset Response acknowledges the Reset Request.

4.2.4.8.1 Sending Reset Responses

Reset Responses are sent by an AP after receiving a Reset Request.

4.2.4.8.2 Format of a Reset Response

The Reset Response carries no message elements. Its purpose is to acknowledge the receipt of the Reset Request.

4.2.4.8.3 Receiving Reset Responses

When an AR receives a Reset Response it is notified that the AP will now reinitialize its operation.

4.2.5 Mobile Session Management

Messages in this section are used by the AR to create session state on the APs.

4.2.5.1 Add Mobile Request

The Add Mobile Request is used by the AR to inform an AP that it should forward traffic from a particular mobile station. The add mobile request may also include specific security parameters that must be enforced by the AP for the particular mobile.

4.2.5.1.1 Sending Add Mobile Requests

When the AR sends an Add Mobile Request, it includes any security parameters that may be required. Further, if the AR's policy is that 802.1X (or WPA) is required, it must set the 802.1X only bit in the Add Mobile message element. An AR that wishes to update a mobile's policy on an AP may be done by simply sending a new Add Mobile Request message.

If 802.1X (or WPA) was established with the mobile station, the AR will need to push a session key the AP must use for encrypting all traffic to the mobile, which is included in the Mobile Session Key message element.

4.2.5.1.2 Format of a Add Mobile Request

When sent by the AP, the Add Mobile Request contains the following message elements:

Add Mobile
Mobile Session Key

4.2.5.1.3 Receiving Add Mobile Requests

When an AP receives an Add Mobile Request, it must first override any existing state it may have for the mobile station in question. The latest Add Mobile Request overrides any previously received messages. If the Add Mobile message element's 802.1X Only bit is set, the AP MUST only allow 802.1X packets to be forwarded to the AR, and must drop any other messages. The AP will be notified via an Add Mobile when it may accept other messages via a new Add Mobile Request from the AR.

If the Mobile Session Key message element was present, the AP MUST add the key to its session key table to ensure that all future packets to the mobile are encrypted using the new key.

4.2.5.2 Add Mobile Response

The Add Mobile Response is used to acknowledge a previously received Add Mobile Request, and includes a Result Code message element which indicates whether an error occured on the AP.

4.2.5.2.1 Sending Add Mobile Response

Add Mobile Response are seny by the AP as a response to the Add Mobile Request.

4.2.5.2.2 Format of a Add Mobile Response

The Add Mobile Response includes the following message element:

Result Code

4.2.5.2.3 Receiving Add Mobile Response

This message requires no special processing, and is only used to acknowledge the Add Mobile Request.

4.2.5.3 Delete Mobile Request

The Delete Mobile Request is used by the AR to inform the AP to terminate service to a particular mobile station.

4.2.5.3.1 Sending Delete Mobile Requests

The AR sends the Delete Mobile Request when it determines that service to the mobile must be terminated. This could occur for various reasons, including for administrative reaons, as a result of the fact that the mobile has roamed to another AP, etc.

4.2.5.3.2 Format of a Delete Mobile Request

The Delete Mobile Request message must include the following message element:

Delete Mobile

4.2.5.3.3 Receiving Delete Mobile Requests

When an AP receives the Delete Mobile Request, it must immediately terminate service to the mobiel station. Any future packets received from the Mobile must result in a deauthenticate message, as specified in xxxxx

4.2.5.4 Delete Mobile Response

The Delete Mobile Response is used to acknowledge a Delete Mobile Request.

4.2.5.4.1 Sending Delete Mobile Response

This message requires no special processing, and is only used to acknowledge the Delete Mobile Request.

4.2.5.4.2 Format of a Delete Mobile Response

The Delete Mobile Response message includes the following message element:

Result Code

4.2.5.4.3 Receiving Delete Mobile Response

No special processing is required for this packet by the AR.

4.2.6 Firmware Management

The Firmware Management messages are used by the AR to ensure that the image being run on each AP is valid.

4.2.6.1 Image Data Request

The Image Data Request is used to update firmware on the AP.

4.2.6.1.1 Sending Image Data Requests

Image Data Requests are exchanged between the AP and the AR to download a new program image to an AP.

4.2.6.1.2 Format of a Image Data Request

When sent by the AP, the Image Data Request contains the following message elements:

Image Download

When sent by the AR, the Image Data Request contains the following message elements:

Image Data

4.2.6.1.3 Receiving Image Data Requests

When an AP or AR receives an Image Data Request it will respond with a Image Data Response.

4.2.6.2 Image Data Response

The Image Data Response acknowledges the Image Data Request.

4.2.6.2.1 Sending Image Data Response

Image Data Responses are sent in response to Image Data Request. Its purpose is to acknowledge the receipt of the Image Data Request packet.

4.2.6.2.2 Format of an Image Data Response

The Image Data Response carries no message elements.

4.2.6.2.3 Receiving Image Data Responses

No action is necessary.

5. LWAPP Message Elements

As previously specified, the LWAPP messages MAY include a message element. The supported message elements are defined in this section.

The allowable values for the Type field are the following:

Description	Type
Result Code	1
AR Address	2
AP Payload	3
AP Name	4
AR Payload	5
Reserved	6
AP WLAN Radio Configuration	7

```
      Rate Set                           8
      Multi-domain capability            9
      MAC Operation                     10
      Reserved                          11
      Tx Power Level                    12
      Direct Sequence Control           13
      OFDM Control                      14
      Supported Rates                   15
      Reserved                          16
      Test                              17
      Reserved                       18-25
      Administrative State              26
      Delete WLAN                       27
      Reserved                       28-29
      AR Name                           30
      Image Download                    31
      Image Data                        32
      Reserved                          33
      Location Data                     34
      Reserved                          35
      Statistics Timer                  36
      Statistics                        37
      Reserved                       38-42
      Certificate                       43
      Session                           44
      Session key                       45
      Reserved                       46-49
      WLAN Payload                      50
      Vendor Specific                   51
      Tx Power                          52
      Add Mobile                        53
      Delete Mobile                     54
      Mobile Session key                55
```


5.1 Result Code

The result code message element value is a 32-bit integer value, indicating the result of the request operation corresponding to the sequence number in the message.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Result Code                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Result Code: The following values are supported

0 Success

1 Failure

5.2 AR Address

The AR address message element is used to communicate the identity of the AR. The value contains two fields, as shown.

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   Reserved    |                  MAC Address                  |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                 MAC Address                   |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Reserved: MUST be set to zero

Mac Address: The MAC Address of the AR

5.3 AP Payload

The AP payload message element is used by the AP to communicate it's current hardware/firmware configuration. The value contains the following fields.

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                      Hardware   Version                       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
     |                      Software   Version                       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                          Boot   Version                       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   Max Radios  | Radios in use |    Encryption Capabilities    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Hardware Version: A 32-bit integer representing the AP's hardware version number

Software Version: A 32-bit integer representing the AP's Firmware version number

Boot Version: A 32-bit integer representing the AP's boot loader's version number

Max Radios: An 8-bit value representing the number of radios (where each radio is identified via the RID field) supported by the AP

Radios in use: An 8-bit value representing the number of radios present in the AP

Encryption Capabilities: This 16-bit field is used by the AP to communicate it's capabilities to the AR. Since most APs support link layer encryption, the AR may opt to make use of these services. This bitfield supports the following values:

1 - Encrypt WEP 104: All packets to/from the mobile station must be encrypted using standard 104 bit WEP.

2 - Encrypt WEP 40: All packets to/from the mobile station must be encrypted using standard 40 bit WEP.

3 - Encrypt WEP 128: All packets to/from the mobile station must be encrypted using standard 128 bit WEP.

4 - Encrypt AES-OCB 128: All packets to/from the mobile station must be encrypted using 128 bit AES OCB [11].

5 - Encrypt TKIP-MIC: All packets to/from the mobile station must be encrypted using TKIP and authenticated using Michael [10].

5.4 AP Name

The AP name message element value is a variable length byte string. The string is NOT zero terminated.

5.5 AR Payload

The AR payload message element is used by the AR to communicate it's current state. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    |                 Hardware  Version ...         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     HW Ver    |                 Software  Version ...         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     SW Ver    |            Stations           |     Limit     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Limit     |            Radios             |   Max Radio   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Max Radio   |
+-+-+-+-+-+-+-+-+
```

Hardware Version: A 32-bit integer representing the AP's hardware version number

Software Version: A 32-bit integer representing the AP's Firmware version number

Stations: A 16-bit integer representing number of mobile stations currently associated with the AR

Limit: A 16-bit integer representing the maximum number of stations supported by the AR

Radios: A 16-bit integer representing the number of APs currently attached to the AR

Max Radio: A 16-bit integer representing the maximum number of APs supported by the AR

5.6 AP WLAN Radio Configuration

The AP WLAN radio configuration is used by the AR to configure a Radio on the AP. The message element value contains the following fields.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Radio ID   |    Reserved   |        Occupancy Limit        |
```



```
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    CFP Per    |      CFP Maximum Duration     |     BSS ID    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                             BSS ID                            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     BSS ID    |         Beacon Period         |    DTIM Per   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Country String                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Reserved: MUST be set to zero

Occupancy Limit: This attribute indicates the maximum amount of time, in TU, that a point coordinator MAY control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value of this attribute SHOULD be 100, and the maximum value SHOULD be 1000

CFP Period: The attribute describes the number of DTIM intervals between the start of CFPs

CFP Maximum Duration: The attribute describes the maximum duration of the CFP in TU that MAY be generated by the PCF

BSSID: The WLAN Radio's MAC Address

Beacon Period: This attribute specifies the number of TU that a station uses for scheduling Beacon transmissions. This value is transmitted in Beacon and Probe Response frames

DTIM Period: This attribute specifies the number of beacon intervals that elapses between transmission of Beacons frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames

Country Code: This attribute identifies the country in which the station is operating. The first two octets of this string is the two character country code as described in document ISO/IEC 3166-1. The third octet MUST be one of the following:

1. an ASCII space character, if the regulations under which the station is operating encompass all environments in the country,

2. an ASCII 'O' character, if the regulations under which the station is operating are for an Outdoor environment only, or

3. an ASCII 'I' character, if the regulations under which the station is operating are for an Indoor environment only

5.7 Rate Set

The rate set message element value is sent by the AR and contains the supported operational rates. It contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |                   Rate Set                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Rate Set: The AR generates the Rate Set that the AP is to include in it's Beacon and Probe messages

5.8 Multi-domain Capability

The multi-domain capability message element is used by the AR to inform the AP of regulatory limits. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   |       First Channel #         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Number of Channels       |     Max Tx Power Level        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Reserved: MUST be set to zero

First Channnel #: This attribute indicates the value of the lowest channel number in the subband for the associated domain country string.

Number of Channels: This attribute indicates the value of the total number of channels allowed in the subband for the associated domain country string.

Max Tx Power Level: This attribute indicates the maximum transmit power, in dBm, allowed in the subband for the associated domain country string.

5.9 MAC Operation

The MAC operation message element is sent by the AR to set the 802.11 MAC parameters on the AP. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   |         RTS Threshold         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Short Retry  |  Long Retry   |    Fragmentation Threshold    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Tx MSDU Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Rx MSDU Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Reserved: MUST be set to zero

RTS Threshold: This attribute indicates the number of octets in an MPDU, below which an RTS/CTS handshake MUST NOT be performed. An RTS/CTS handshake MUST be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size MUST have the effect of turning off the RTS/CTS handshake for frames of Data or Management type transmitted by this STA. Setting this attribute to zero MUST have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute MUST be 2347

Short Retry: This attribute indicates the maximum number of transmission attempts of a frame, the length of which is less than or equal to RTSThreshold, that MUST be made before a failure condition is indicated. The default value of this attribute MUST be 7

Long Retry: This attribute indicates the maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that MUST be made before a failure condition is indicated. The default value of this attribute MUST

be 4

Fragmentation Threshold: This attribute specifies the current maximum size, in octets, of the MPDU that MAY be delivered to the PHY. An MSDU MUST be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU MUST be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute MUST be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and MUST never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute MUST never be less than 256

Tx MSDU Lifetime: This attribute speficies the elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU MUST be terminated. The default value of this attribute MUST be 512

Rx MSDU Lifetime: This attribute specifies the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU MUST be terminated. The default value MUST be 512

5.10 Tx Power Level

The Tx power level message element is sent by the AP and contains the different power levels supported. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |  Num Levels   |        Power Level [n]        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Num Levels: The number of power level attributes

Power Level: Each power level fields contains a supported power level, in mW.

5.11 Direct Sequence Control

The direct sequence control message element is a bi-directional element. When sent by the AP, it contains the current state. When sent by the AR, the AP MUST adhere to the values. This element is only used for 802.11b radios. The value has the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   | Current Chan  |  Current CCA  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Energy Detect Threshold                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Reserved: MUST be set to zero

Current Channel: This attribute contains the current operating frequency channel of the DSSS PHY.

Current CCA: The current CCA method in operation. Valid values are:

1 - energy detect only (edonly)

2 - carrier sense only (csonly)

4 - carrier sense and energy detect (edandcs)

8 - carrier sense with timer (cswithtimer)

16 - high rate carrier sense and energy detect (hrcsanded)

Energy Detect Threshold The current Energy Detect Threshold being used by the DSSS PHY

5.12 OFDM Control

The OFDM control message element is a bi-directional element. When sent by the AP, it contains the current state. When sent by the AR, the AP MUST adhere to the values. This element is only used for 802.11a radios. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   | Current Chan  |  Band Support |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         TI Threshold                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Reserved: MUST be set to zero

Current Channel: This attribute contains the current operating frequency channel of the OFDM PHY.

Band Supported: The capability of the OFDM PHY implementation to operate in the three U-NII bands. Coded as an integer value of a three bit field as follows:

Bit 0 - capable of operating in the lower (5.15-5.25 GHz) U-NII band

Bit 1 - capable of operating in the middle (5.25-5.35 GHz) U-NII band

Bit 2 - capable of operating in the upper (5.725-5.825 GHz) U-NII band

For example, for an implementation capable of operating in the lower and mid bands this attribute would take the value

TI Threshold: The Threshold being used to detect a busy medium (frequency). CCA MUST report a busy medium upon detecting the

RSSI above this threshold

5.13 Supported Rates

The supported rates message element is sent by the AP to indicate the rates that it supports. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |                 Supported Rates               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio

Supported Rates: The AP includes the Supported Rates that it's

hardware supports. The format is identical to the Rate Set message element

5.14 Test

The test message element is used as padding to perform MTU discovery, and MAY contain any value, of any length.

5.15 Administrative State

The administrative event message element is used to communicate the state of a particular radio. The value contains the following fields.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |  Admin State  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Admin State: An 8-bit value representing the administrative state of the radio. The following values are supported:

0 - Enabled

1 - Disabled

5.16 Delete WLAN

The delete WLAN message element is used to inform the AP that a previously created WLAN is to be deleted. The value contains the following fields.

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
      |    Radio ID   |             WLAN ID           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio

WLAN ID: A 16-bit value specifying the WLAN Identifier

5.17 AR Name

The AR name message element contains an ASCII representation of the AR's identity. The value is a variable length byte string. The string is NOT zero terminated.

5.18 Image Download

The image download message element is sent by the AP to the AR and contains the image filename. The value is a variable length byte string. The string is NOT zero terminated.

5.19 Image Data

The image data message element value contains the following fields.

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Opcode    |           Checksum            |  Image Data   |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                          Image Data �                         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Opcode: An 8-bit value representing the transfer opcode. The following values are supported:

3 - Image data is included

5 - An error occurred. Transfer is aborted

Checksum: A 16-bit value containing a checksum of the image data that follows

Image Data: A variable length firmward data

5.20 Location Data

The location data message element is a variable length byte string containing user defined location information (e.g. �Next to Fridge�). The string is NOT zero terminated.

5.21 Statistics Timer

The statistics timer message element value is used by the AR to inform the AP of the frequency which it expects to receive updated statistics.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Statistics Timer       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Statistics Timer: A 16-bit unsigned integer indicating the time, in seconds

5.22 Statistics

The statistics message element is sent by the AP to transmit it's current statistics. The value contains the following fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |               Tx Fragment Count               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Tx Fragment Cnt|               Multicast Tx Count              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Mcast Tx Cnt  |                  Failed Count                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Failed Count  |                  Retry Count                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Retry Count  |             Multiple Retry Count              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Multi Retry Cnt|             Frame Duplicate Count             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Frame Dup Cnt |               RTS Success Count               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RTS Success Cnt|               RTS Failure Count               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RTS Failure Cnt|               ACK Failure Count               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|ACK Failure Cnt|               Rx Fragment Count               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Rx Fragment Cnt|               Multicast RX Count              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Mcast Rx Cnt  |                FCS Error  Count               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| FCS Error  Cnt|                 Tx Frame Count                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tx Frame Cnt  |                    Reserved                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Reserved   |
+-+-+-+-+-+-+-+-+
```


Radio ID: An 8-bit value representing the radio

Tx Fragment Count: A 32-bit value representing the number of fragmented frames transmitted.

Multicast Tx Count: A 32-bit value representing the number of multicast frames transmitted.

Failed Count: A 32-bit value representing the transmit excessive retries.

Retry Count: A 32-bit value representing the number of transmit retries.

Multiple Retry Count: A 32-bit value representing the number of transmits that required more than one retry.

Frame Duplicate Count: A 32-bit value representing the duplicate frames received.

RTS Success Count: A 32-bit value representing the number of successful Ready To Send (RTS).

RTS Failure Count: A 32-bit value representing the failed RTS.

ACK Failure Count: A 32-bit value representing the number of failed acknowledgements.

Rx Fragment Count: A 32-bit value representing the number of fragmented frames received.

Multicast RX Count: A 32-bit value representing the number of multicast frames received.

FCS Error Count: A 32-bit value representing the number of FCS failures.

Reserved: MUST be set to zero

5.23 Antenna

The antenna message element is communicated by the AP to the AR to provide information on the antennas available. The AR MAY use this element to reconfigure the AP's antennas. The value contains the following fields.

```
  0                   1                   2                   3
```



```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Radio ID   |   Diversity   |    Reserved    |  Antenna Cnt |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Antenna Selection [0..N]                   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio

Diversity: An 8-bit value specifying whether the antenna is to provide receive diversity. The following values are supported:

0 - Disabled

1 - Enabled (may only be true if the antenna can be used as a receive antenna)

Reserved: MUST be set to zero

Antenna Count: An 8-bit value specifying the number of Antenna Selection fields.

Antenna Selection: A 32-bit value representing the antenna type. The following values are supported:

1 - Sectorized (Left)

2 - Sectorized (Right)

3 - Omni

5.24 Certificate

The certificate message element value is a byte string containing a PKCS #5 certificate [5].

5.25 Session ID

The session ID message element value contains a randomly generated [6] unsigned 32-bit integer.

5.26 Session Key Payload

The Session Key Payload message element is sent by the AR to the AP and includes the randomly generated session key, which is used to protect the LWAPP control messages. More details are available in appedix A. The value contains the following fields.


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session Key                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session Key                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session Key                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session Key                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Session ID: A 32-bit value representing the session which this session key is related to

Session Key: A 128-bit value randomly generated session key [6]

5.27 WLAN Payload

The WLAN payload message element is used by the AR to define a wireless LAN on the AP. The value contains the following format:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |         WLAN Capability       |    WLAN ID    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    WLAN ID    |         SSID ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio

WLAN Capability: A 16-bit value containing the capabilities to be advertised by the AP within the Probe and Beacon messages.

WLAN ID: A 16-bit value specifying the WLAN Identifier

SSID: The SSID attribute is a variable length byte string containing the SSID to be advertised by the AP. The string is NOT zero terminated.

5.28 Vendor Specific Payload

The Vendor Specific Payload is used to communicate vendor specific information between the AP and the AR. The value contains the following format:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Vendor Identifier                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Element ID           |    Value...   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Vendor Identifier: A 32-bit value containing the IANA assigned �SMI Network Management Private Enterprise Codes [7]

Element ID: A 16-bit Element Idenfier which is managed by the vendor.

Element ID: Value The value associated with the vendor specific element.

5.29 Tx Power

The Tx power message element value is bi-directional. When sent by the AP, it contains the current power level of the radio in question. When sent by the AR, it contains the power level the AP MUST adhere to.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |    Reserved   |       Current Tx Power        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio to configure

Reserved: MUST be set to zero

Current Tx Power: This attribute contains the transmit output power in mW

5.30 Add Mobile

The Add Mobile message element is used by the AR to inform the AP that it should allow traffic from/to a particular mobile station.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |        Association ID         |  MAC Address  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          MAC Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  MAC Address  | Preamble Mode |    WLAN ID    |Supported Rates|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Supported Rates                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  802.1X Only  |
+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio

Association ID: A 16-bit value specifying the 802.11 Association Identifier

MAC Address: The mobile station's MAC Address

Preamble Mode: This field is set by the AR to inform the AP whether short or long preamble should be used with the mobile station. The following values are supported:

0 - Long Preamble: Long preamble is to be used by the AP when communicating with the mobile station.

1 - Short Preamble: Short preamble is to be used by the AP when communicating with the mobile station.

WLAN ID: A 16-bit value specifying the WLAN Identifier

Supported Rates: The supported rates to be used with the mobile station.

802.1X Only: The AR sets this field to one (1) during the authentication phase to inform the AP to only allow EAP frames through.

5.31 Delete Mobile

The Delete Mobile message element is used by the AR to inform an AP that it should no longer provide service to a particular mobile station.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Radio ID   |                 MAC Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   MAC Address                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio

MAC Address: The mobile station's MAC Address

5.32 Mobile Session Key

The Mobile Session Key Payload message element is sent when the AR determines that encryption of a mobile station must be performed in the AP. This message element MUST NOT be present without the Add Mobile (see Section 5.30)message element, and MUST NOT be sent if the AP had not specifically advertised support for the requested encryption scheme (see Section 5.3).

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Mac Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Mac Address          |       Encryption Policy       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Encryption Policy       |         Session Key...        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

MAC Address: The mobile station's MAC Address

Encryption Policy: The policy field informs the AP how to handle packets from/to the mobile station. The following values are supported:

0 - Encrypt WEP 104: All packets to/from the mobile station must be encrypted using standard 104 bit WEP.

1 - Clear Text: All packets to/from the mobile station do not

require any additional crypto processing by the AP.

2 - Encrypt WEP 40: All packets to/from the mobile station must be encrypted using standard 40 bit WEP.

3 - Encrypt WEP 128: All packets to/from the mobile station must be encrypted using standard 128 bit WEP.

4 - Encrypt AES-OCB 128: All packets to/from the mobile station must be encrypted using 128 bit AES OCB [11].

5 - Encrypt TKIP-MIC: All packets to/from the mobile station must be encrypted using TKIP and authenticated using Michael [10].

Session Key: The session key the AP is to use when encrypting traffic to/from the mobile station.

6. LWAPP Configuration Variables

An AP or AR that implements LWAPP discovery MUST allow for the following variables to be configured by system management; default values are specified so as to make it unnecessary to configure any of these variables in many cases.

6.1 MaxDiscoveryInterval

The maximum time allowed between sending discovery requests from the interface, in seconds. Must be no less than 2 seconds and no greater than 180 seconds.

Default: 20 seconds.

6.2 MaxDiscoveries

The maximum number of discovery requests that will be sent after an AP boots.

Default: 10

6.3 SilentInterval

The minimum time, in seconds, an AP MUST wait after failing to receive any responses to its discovery requests, before it MAY again send discovery requests.

Default: 30

6.4 NeighborDeadInterval

The minimum time, in seconds, an AP MUST wait without having received echo replies to its echo responses, before the destination for the echo replies may be considered dead. Must be no less than 2*EchoInterval seconds and no greater than 240 seconds.

Default: 60

6.5 EchoInterval

The minimum time, in seconds, between sending echo requests to the AR with which the AP has joined.

Default: 30

6.6 DiscoveryInterval

The minimum time, in seconds, that an AP MUST wait after receiving a discovery reply, before sending a join request.

Default: 5

7. LWAPP Transport Layer

The LWAPP protocol can operate at layer 2 or 3. For layer 2 support, the LWAPP frames are carried in a native Ethernet frame. As such, the protocol is not routable and depends upon layer 2 connectivity between the AP and the AR. Layer 3 support is provided by encapsulating the LWAPP frames within UDP.

7.1 Layer 2

This section describes how the LWAPP protocol is provided over native ethernet frames. All LWAPP frames are encapsulated within 802.3 frames, whose fields are defined below.

7.1.1 Source Address

A MAC address belonging to the interface from which this message is sent. If multiple source addresses are configured on an interface, then the one chosen is implementation dependent.

7.1.2 Destination Address

A MAC address belonging to the interface to which this message is to be sent. This destination address MAY be either an individual address or a multicast address, if more than one destination interface is intended.

7.1.3 Ethertype

The Ethertype field is set to 0x88bb.

7.1.4 AR Discovery

When run over Ethernet, the LWAPP protocol is restricted to a specific Ethernet segment. The AR discovery mechanism used with this transport is for the Discovery Request message to be transmitted to a broadcast address. The ARs will receive this message and reply based on their policy.

7.1.5 Extended LWAPP Message Format

When LWAPP is run over a layer 2 interface, the base LWAPP header is extended to include fields that are only useful when run over this transport. The following figure and associated text describes the new fields.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|VER| RID |C|F|L|    Frag ID    |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Ctl/Stat           |   Payload...  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

7.1.5.1 Flags Field

The first byte contains several flag fields. The following flags are only used when LWAPP is run over a layer 2 interface:

7.1.5.2 C Bit

The C bit indicates whether this packet carries data or control information. When this bit is 0, the packet carries an encapsulated data frame. When this bit is 1, the packet carries control information for consumption by the addressed destination.

7.1.5.3 F Bit

The F bit indicates whether this packet is a fragment. When this bit is 1, the packet is a fragment and MUST be combined with the other corresponding fragments to reassemble the complete information exchanged between the AP and AR.

7.1.5.4 L Bit

The L bit is valid only if the 'F' bit is set and indicates whether the packet contains the last fragment of a fragmented exchange between AP and AR. When this bit is 1, the packet is not the last fragment. When this bit is 0, the packet is the last fragment.

7.1.5.5 Fragment ID

The Fragment ID is a value assigned to each group of fragments making up a complete set. The value of Fragment ID is incremented with each new set of fragments. The Fragment ID wraps to zero after the maximum value has been used to identify a set of fragments. LWAPP only supports up to 2 fragments.

7.2 Layer 3

This section defines how LWAPP makes use of UDP transport between the AP and the AR.

7.2.1 Framing

Communication between AP and AR is established according to the standard UDP client/server model. The connection is initiated by the AP (client) to the well-known UDP port of the AR (server) used for control messages. This UDP port number of the AR is TBD.

7.2.2 Fragmentation/Reassembly

When LWAPP is implemented at L3, the transport layer uses IP fragmentation to fragment and reassemble LWAPP messages that are longer than MTU size used by either AP or AR. The details of IP fragmentation are covered in [3].

[ed: IP fragmentation may raise security concerns and bring additional configuration requirements for certain firewalls and NATs. One alternative is to re-use the layer 2 (application layer) fragmentation reassembly. Comments are welcomed.]

7.2.3 Multiplexing

LWAPP messages convey control information between AP and AR, as well as, 802.11 data frames or 802.11 management frames. As such, LWAPP messages needs to be multiplexed in the transport sub-layer and be delivered to the proper software entities in the endpoints of the protocol.

In case of Layer 3 connection, multiplexing is achieved by use of different UDP ports for control and data packets.

As part of Join procedure, the AP and AR may negotiate different UDP ports, as well as, different IP addresses for data or session management messages. [ed: details on how to communicate this information in the protocol is still missing].

In the event the AP and AR are separated by a NAT, with the AP using private IP address space, it is the responsibility of the NAT to manage appropriate UDP port mapping.

7.2.4 AR Discovery

When LWAPP is run over routed IP network, the AP and the AR do not need to reside in the same IP subnet (broadcast domain). However, in the event the peers reside on separate IP subnets, there must exist a mechanism for the AP to discover the AR.

As the AP attempts to establish communication with the AR, it sends the Discovery Request message and receives the corresponding reply

message from the AR. The AP may send the Discovery Request message to either limited broadcast IP address (255.255.255.255) or to the unicast IP address of the AR. Upon receipt of the message, the AR issues a Discovery Reply message to the IP address of the AP, regardless of whether Discovery Request was sent as a broadcast or unicast message.

Whether the AP uses a limited IP broadcast or unicast IP address is implementation dependent.

In order for the AP to use a unicast address, it must first obtain the IP address of the AR. The configuration of the AR's address in the AP is implementation dependent and outside the scope of this document. However, some possibilities is to make use of a vendor specific DHCP option, DNS name resolution, or even static provisioning of the AR's IP address in non-volatile storage.

8. Light Weight Access Protocol Constants

MAX_RESPONSE_DELAY	2 seconds
MAX_SOLICITATION_DELAY	1 second
SOLICITATION_INTERVAL	3 seconds
MAX_SOLICITATIONS	3 transmissions

9. Security Considerations

LWAPP uses public key cryptography to ensure trust between the AP and the AR. During the Join phase, the AR generates a session key, which is used to secure all future control messages. The AP does not participate in the key generation, but public key cryptography is used to authenticate the resulting key material. A secured delivery mechanism to place the certificate in the devices is required. In order to maximize session key security, the AP and AR periodically update the session keys, which are encrypted using public key cryptography. This ensures that a potentially previously compromised key does not affect the security of communication with new key material.

One question that periodically arises is why the Join Request is not signed. It was felt that requiring a signature in this messages was not required for the following reasons:

1. The Join Request is replayable, so requiring a signature doesn't provide much protection unless the switches keep track of all previous Join Requests from a given AP. One alternative would have been to add a timestamp, but this introduces clock synchronization issues. Further, authentication occurs in a later exchange anyway (see point 2 below).

2. The AP is authenticated by virtue of the fact that it can decrypt and then use the session keys (encrypted with its own public key), so it *is* ultimately authenticated.

3. A signed Join Request provides a potential Denial of Service attack on the AR, which would have to authenticate each (potentially malicious) message.

10. IPR Statement

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

References

[1] "Advanced Encryption Standard (AES)", November 2001, <FIPS PUB 197>.

[2] "Counter with CBC-MAC (CCM)", January 2003, <ftp://ftp.isi.edu/internet-drafts/draft-housley-ccm-mode-02.txt>.

[3] "IP DATAGRAM REASSEMBLY ALGORITHMS", July 1992, <ftp://ftp.isi.edu/in-notes/rfc815>.

[4] "Key words for use in RFCs to Indicate Requirement Levels", March 1997, <ftp://ftp.isi.edu/in-notes/rfc2119>.

[5] "PKCS #5: Password-Based Encryption Standard. Version 1.5", November 1993.

[6] "Randomness Recommendations for Security", December 1994, <ftp://ftp.isi.edu/in-notes/rfc1750>.

[7] "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", January 2002, <ftp://ftp.isi.edu/in-notes/rfc3232>.

[8] "The Internet Standards Process Revision 3", October 1996, <ftp://ftp.isi.edu/in-notes/rfc2026>.

[9] "Mobility Related Terminology", April 2003, <ftp://ftp.isi.edu/internet-drafts/draft-ietf-seamoby-terminology-04.txt>.

[10] "WiFi Protected Access (WPA) rev 1.6", April 2003.

[11] "IEEE Std 802.11i/3.0: Specification for Enhanced Security", November 2003.

Authors' Addresses

Pat R. Calhoun
Airespace
110 Nortech Parkway
San Jose, CA 95134

Phone: +1 408-635-2000
EMail: pcalhoun@airespace.com

Bob O'Hara
Airespace
110 Nortech Parkway
San Jose, CA 95134

Phone: +1 408-635-2025
EMail: bob@airespace.com

Scott Kelly
Airespace
110 Nortech Parkway
San Jose, CA 95134

Phone: +1 408-635-2022
EMail: skelly@airespace.com

Rohit Suri
Airespace
110 Nortech Parkway
San Jose, CA 95134

Phone: +1 408-635-2026
EMail: rsuri@airespace.com

Daichi Funato
DoCoMo USA Labs
180 Metro Drive, Suite 300
San Jose, CA 95110

Phone: +1 408-451-4736
EMail: funato@docomolabs-usa.com

Michael Vakulenko
Legra Systems, Inc.
3 Burlington Woods Drive
Burlington, MA 01803

Phone: +1 781-272-8400
EMail: michaelv@legra.com

Appendix A. Session Key Generation

Note: This version only defines a certificate based mechanism to secure traffic between the AP and the AR. A shared-secret mechanism will be added in a future version.

A.1 Securing AP-AR communications

While it is generally straightforward to produce network installations in which the communications medium between the AP and AR is not accessible to the casual user (e.g. these LAN segments are isolated, no RJ45 or other access ports exist between the AP and the AR), this will not always be the case. Furthermore, a determined attacker may resort to various more sophisticated monitoring and/or access techniques, thereby compromising the integrity of this connection.

In general, a certain level of threat on the local (wired) LAN is expected and accepted in most computing environments. That is, it is expected that in order to provide users with an acceptable level of service and maintain reasonable productivity levels, a certain amount of risk must be tolerated. It is generally believed that a certain perimeter is maintained around such LANs, that an attacker must have access to the building(s) in which such LANs exist, and that they must be able to "plug in" to the LAN in order to access the network.

With these things in mind, we can begin to assess the general security requirements for AR-AP communications. While an in-depth security analysis of threats and risks to these communication is beyond the scope of this document, some discussion of the motivation for various security-related design choices is useful. The assumptions driving the security design thus far include the following:

- AP-AR communications take place over a wired connection which may be accessible to a sophisticated attacker

- access to this connection is not trivial for an outsider (i.e. someone who does not "belong" in the building) to access

- if authentication and/or privacy of end to end traffic for which the AP and AR are intermediaries is required, this may be provided via IPsec.

- privacy and authentication for at least some AP-AR control traffic is required (e.g. WEP keys for user sessions, passed from AR to AP)

- the AR can be trusted to generate strong cryptographic keys

AR-AP traffic can be considered to consist of two types: data traffic (e.g. from or to an end user), and control traffic which is strictly between the AR and AP. Since data traffic may be secured using Ipsec (or some other end-to-end security mechanism), we confine our solution to control traffic. The resulting security consists of two components: an authenticated key exchange, and control traffic security encapsulation. The security encapsulation is accomplished using CCM, described in [2]. This encapsulation provides for strong AES-based authentication and encryption. The exchange of cryptographic keys used for CCM is described below.

A.2 Authenticated Key Exchange

The AR and AP accomplish mutual authentication and a cryptographic key exchange in a single round trip using the JOIN request/response pair. To accomplish this, the AP includes its identity certificate (see Section 5.24) and a randomly-generated session ID (see Section 5.25) which functions as a cryptographic nonce in the JOIN request. The AR verifies the AP's certificate, and replies with its own identity certificate, and a signed concatenation of the session ID and and encrypted cryptographic session key. This exchange is detailed below.

Before proceeding, we define the following notation:

- Kpriv - the private key of a public-private key pair.

- Kpub - the public key of the pair

- M - a clear-text message

- C - a cipher-text message.

- PKCS1(z) - the PKCS#1 encapsulation of z

- E-x{Kpriv, M} - encryption of M using X's private key

- E-x{Kpub, M} - encryption of M using X's public key

- S-x{M} - a digital signature over M produced by X o V-x{S-x, M} - verification of X's digital signature over M

o D-x{Kpriv, C} - decryption of C using X's private key

o D-x{Kpub, C} - decryption of C using X's public key

o Certificate-AR - AR's Certificate

o Certificate-AP - AP's Certificate

When the AR receives the SessionID value along with the AP's certificate, it constructs the reply payload as follows:

o Randomly generate enough key material to produce an encryption key and an authentication hash key (xx bytes in length). [TBD: detailed key material generation instructions]

o Compute C1 = E-ap{ Kpub , PKCS1(KeyMaterial)}; this encrypts the PKCS#1-encoded key material with the public key of the AP, so that only the AP can decrypt it and determine the session keys.

o Compute S1 = S-ar{SessionID|C1}; this computes the AR's digital signature over the concatenation of the nonce and the encrypted key material, and can be verified using the public key of the AR, "proving" that the AR produced this; this forms the basis of trust for the AP with respect to the source of the session keys.

o AR sends (Certificate-AR, C1, S1, SessionID) to AP

o AP verifies that SessionID matches an outstanding request

o AP verifies authenticity of Certificate-AR

o AP computes V-ar{S1, SessionID|C1}, verifying the AR's signature over the session identifier and the encrypted key material

o AP computes PKCS1(KeyMaterial) = D-ar{ Kpriv , C1}, decrypting the session keys using its private key; since these were encrypted with the AP's public key, only the AP can successfully decrypt this.

  KeyMaterial is divided into the encryption key and the HMAC key [TBD: say how] From this point on, all control protocol payloads between the AP and AR are encrypted and authenticated. The related payloads are described in the sections above.

A.3 Refreshing Cryptographic Keys

Since AR-AP associations will tend to be relatively long-lived, it is sensible to periodically refresh the encryption and authentication keys; this is referred to as "rekeying". When the key lifetime reaches 95% of the configured value, the rekeying will proceed as follows:

- o AP generates a fresh SessionID value, and constructs a TLV payload of type SESSION which contains new SessionID and sends it in KEY-UPDATE message to AR.

- o When the AR receives KEY-UPDATE request with SessionID it constructs the reply payload as follows:

  i) Randomly generate enough key material to produce an encryption key and an authentication hash key (xx bytes in length). [TBD:detailed key material generation instructions]

  ii) Compute C1 = E-ap{ Kpub , PKCS1(KeyMaterial)}; this encrypts the PKCS#1-encoded key material with the public key of the AP, so that only the AP can decrypt it and determine the session keys.

  iii) Compute S1 = S-ar{SessionID|C1}; this computes the AR's digital signature over the concatenation of the sessionId and the encrypted key material, and can be verified using the public key of the AR, "proving" that the AR produced this; this forms the basis of trust for the AP with respect to the source of the session keys.

  iv) AR then sends a KEY-UPDATE-RSP message to the AP using the new session values.

- o AP must maintain session state for the original SessionID and keys until it receives the KEY-UPDATE-RSP, at which time it clears the old session.

- o If AP does not receive the KEY-UPDATE-RSP within a reasonable period of time (1 minute?), it will resend the original request and reset its response timer. If no response occurs by the time the original session expires, the AP will delete the new and old session information, and initiate the DISCOVER process anew.

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

Network Working Group M. Mani
Internet-Draft Avaya Inc.
Expires: April 19, 2004 B. O'Hara
Airespace
L. Yang
Intel Corp.
October 20, 2003

Architecture for Control and Provisioning of Wireless Access Points(CAPWAP)
draft-mani-ietf-capwap-arch-00

Status of this Memo

Copyright Notice

Abstract

While conventional wisdom has it that Wireless Access Points are strictly Layer 2 bridges, such devices today perform some higher layer functions of routers or switches in wired Infrastructure in addition to bridging the wired and wireless networks. For example, in 802.11 networks, Access Points can function as Network Access Servers. For this reason, Access Points have IP addresses and can function as IP devices.

This Document analyzes WLAN (Wireless LAN) functions and services; and describes a flexible balance of such AP (Access Point) functions as allowed in the Standards and practiced in the industry, to be meaningfully split between lightweight Access Point (LAP) framework

and AP Controllers or AR (Access Router) framework managing them.

Table of Contents

1. Introduction

1.1 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [7].

1.2 CAPWAP Purpose and Scope

The purpose of CAPWAP work is to define the framework reflecting the architectural trend that delegates and aggregates selected WLAN functions and services from APs to ARs to enhance WLAN resource management. On the basis of such definition CAPWAP aims to provide a secure protocol to enable AP-to-AR communications and AP provisioning & management.

1.3 Document Organization

Overview section describes the IEEE 802.11 WLAN architecture and services in brief followed by AP-AR network topological considerations leading to CAPWAP motivation.

Subsequent section describes the CAPWAP architecture and its components.

The section that follows discusses related research work and an applicable standards topology.

The document concludes with Security Considerations which are also discussed in Architecture.

2. Terminology

LWAP: Lightweight Access Point

AB/AR: Access Bridges/Routers

AC: Access Controllers

AP: access point

BSS: basic service set

ESS: extended service set

SSID: service set identifier

WLAN: wireless local area network

RSN: robust security network

TSN: transition security network

PMK: pair-wise master key

PTK: pair-wise transient key

TK: temporal key

GMK: group master key

GTK: group transient key

KCK: key confirmation key

KEK: key encryption key

PSK: pre-shared key

WEP: wired equivalent privacy

Throughout the document the terminologies of AR (Access Router), AC (Access Controller) and AB (Access Bridge) are used synonymously in contexts of allowable network topology arguments. In other cases the distinction is called out explicityl.

However, at the outset AC is to be assumed the generic term for the entity with which an AP registers or associates - which terms will be qualified later in the CAPWAP architecture sections (Section 4).

AR is called out in the context that the Access Controller that an AP associates with is over an allowed L3 cloud between the wired network backend of APs and the ACs.

Access Bridge (or WLAN switch) is called out in the context of such network cloud or connectivity may be over a predominantly L2 network.

It may be observed in following sections that the proposed architecture chooses to stay agnostic and equivalent to either Network Protocol and focuses on the interface and generic encapsulation that shall allow for both. The Protocol MAY end up specifying merely for IP.

3. Overview

Prior to setting out on details, a snapshot of WLAN standards are in order to put the CAPWAP motivation and standardization benefits in perspective, particularly when the required interfaces appear in the landscape bordering L2 and L3 standards scope.

3.1 The IEEE 802.11 in Brief

The IEEE 802.11 standard for wireless local area networks [1] specifies a MAC protocol, several PHYs, and a MAC management protocol. Each of these operates over the air, between two or more 802.11 devices. 802.11 also describes how mobile devices can associate together into a basic service set (BSS), the rough equivalent of a single broadcast domain or a segment of a bridged Ethernet LAN. A BSS is identified by a common service set identifier (SSID) or name. An SSID is an arbitrary byte string, up to 32 bytes long, though most implementations utilize ASCII strings for readability. 802.11 also describes the functionality of a specific device, called an access point (AP), that translates frames between mobile 802.11 devices and hosts on a wired network. When more than one AP is connected via a broadcast layer 2 network and all are using the same SSID, an extended service set (ESS) is created. An ESS is also similar to a single broadcast domain, where a mobile device associated with one AP can successfully ARP for the address of a mobile device associated with any other AP in the ESS. Within an ESS, a mobile station can roam from one AP to another through only layer 2 transitions coordinated by the 802.11 MAC management protocol. Higher layer protocols, including IP are unaware that the network attachment point of the mobile device has moved.

The 802.11 working group is currently proceeding on work related to layer 2 security and quality of service. The 802.11i task group is addressing the security issues of the original 802.11 standard in the areas of authentication and encryption. This work refers to other standards, including 802.1X Port Based Access Control [14] and the Extensible Authentication Protocol [9]. The 802.11e task group is addressing layer 2 quality of service items through extending the access method, frame definitions, and MAC management protocol of the original standard. This work refers to the 802.1Q [15] standard.

802.11 PHYs are wireless, by definition, and principally use radio technology for communication. An aspect of an 802.11 WLAN that is not addressed by the standard is the necessity to manage the self-interference of one AP when operating on a radio channel equal to or near the radio channel of another AP within reception range. Managing self-interference within the WLAN involves both measurement of the level of interference, as well as control of the transmit power and transmitting channel in each of the APs. Work currently in process in the 802.11k task group is addressing the issue of radio resource measurement, which will provide the information on level of interference, among other things.

Some definitions of 802.11 terminology is in order, since it is unique to the 802.11 standard.

* "Distribution" is the service of forwarding MSDUs for an associated station by an AP. As it is described in 802.11, distribution by an AP is providing sufficient information to enable a frame received from an associated station to be successfully delivered to its proper destination. For the most part, this involves translating the frame format from 802.11 to Ethernet (typically) and removing any SNAP encapsulation that was applied to the 802.11 frame, due to its lack of an equivalent to the Ethertype field. This is similar to standard bridging, except that 802.11 APs are not 802.1D bridges. APs typically do not implement spanning tree protocols or algorithms. They are considered to be edge devices, connected only to leaf nodes with no further bridging taking place down stream from them. This is not always a valid assumption and can sometimes result in unanticipated bridging loops.

* "Integration" is a concept unique to 802.11 that is a result of the underlying architecture. 802.11 considers that the individual APs that make up a WLAN, an extended service set (ESS) in 802.11 terminology, are connected by a closed system, called the distribution system. Only frames that are "within" the ESS are carried by the distribution system. This includes frames that are moving from one AP to another for delivery to a mobile station, frames received from outside the ESS for delivery to a mobile station, and frames from a mobile station to be delivered outside the ESS. Connecting the closed distribution system to the outside world is a "portal". The portal is the single point at which the distribution system exchanges frames with the network outside of the ESS.

The problem with the 802.11 architecture, or maybe just with the AP implementations, is that AP implementations do not adhere to this architecture. An AP typically implements both the distribution and integration services, and the portal function, inside the skin of the AP. In this sense, every AP is its own, isolated ESS and no APs actually implement the architecture described in the standard. When a set of APs is connected together to create a WLAN, what is actually created is a set of independent ESSs that happen to communicate, in spite of the implementation.

In addition to the 802.11 standard, the 802.11 working group produced a recommended practice for inter-AP communication, 802.11F [12]. The recommended practice describes the use of a new application protocol, the Inter-AP Protocol (IAPP), carried on UDP or TCP. It permits APs to exchange information about roaming mobile devices, including an envelope for general context transfer purposes, and to push layer 2 keying information to neighboring APs in preparation for the roaming of mobile devices to those neighboring APs. The recommended practice specifies the use of 802.2 XID frames for updating layer 2 devices when a mobile device's point of attachment to the network has changed due to a roaming event. 802.11F also specifies the use of RADIUS for the authentication of one AP to another and, along with portions of the IAPP protocol, to establish secure IAPP packets exchanged between participating APs.

The IAPP is not applicable to this architecture, though it may be implemented in the access controller for communication with other access controllers as 802.11 intended it to be used between individual APs. It is not applicable within the CAPWAP architecture because, presumably, the communications defined by CAPWAP would be internal to the access controller and not require such a protocol to be utilized.

3.2 CAPWAP Motivation

As evidenced over the past few months, there is overwhelming support in the market for a new WLAN architecture. This architecture moves much of the functions that would reside in a traditional access point (AP) to a centralized access router (AR). Some of the benefits that come out of this new architecture include:

o Ease of Use: By centrally managing a WLAN as a system rather than as a series of discrete components, management and control of the WLAN is much easier

o Increased Security: Having a centralized AR enforce policies and being able to detect potential threats across a much larger RF domain increases the security of the network.

o Enhanced Mobility: By terminating the WLAN "management" protocol in the AR, these messages may be used as "mobility triggers", providing mobility across an RF domain without the need for any client software.

o Quality of Service: By allowing the centralized AR manage the RF links, offers systemic perspective to perform efficient load balancing across multiple Access Points - thus increasing the efficiency of the wireless network. It also offers scope to have higher layer applications influence roaming and placement policies in a streamlined manner.

All of the above can be providing by terminating the 802.11 management frames in the AR. This approach is also commonly referred to as Split AP, where the real-time components of the 802.11 protocol are handled in the Access Point, while the access control components of the 802.11 protocol terminate in the Access Router.

Having a module in the AR that understands 802.11 management frames and 802.11 WLANs will provide much better control and optimization of the WLAN operation than will an abstract, protocol-agnostic control module. Adding support to CAPWAP/LWAPP for other wireless technologies then becomes a task of encapsulating the new frames and adding a new control module to the AR to handle the new technology. Presumably, the LWAPP protocol and CAPWAP architecture will need little, if any change.

3.3 AP to AR Network Topology Considerations

APs and ARs are linked directly as required by some architectures. Among such classifications

1. ARCH0: The classic AP is at one of the spectrum interfaces to the Infrastructure Network cloud with no specific connectivity to a controller. In this case the AP can be considered to have a self-contained controller possibly communicating with other APs in the ESS to form a WDS.

2. ARCH1: APs which defer all WLAN functions other than real-time services (Section 4.1) create a vastly different paradigm of vertical (real-time frontend AP and aggregated backend AC) functional distribution calling for a trust model between the two and a discovery process of AC by AP. The latter (discovery) is accentuated when the connectivity is through a cloud and there's potential for m-to-n correspondence of AP-AR.

3. ARCH2: APs which tend to shift some normally real-time functions as well to the backend with benefits such as extending OTA (over-the-air) protection for AP-AR thus allowing for an extended Trust Model for client data.

4. ARCH3: There's the case which carries (3) to render the AC as a single "AP-switch" treating all connected APs as smart antennae.

While, at the outset, the architectures seem at wider variance, the varied market requirements of

1. deployment scope

2. scalability

3. performance and

4. end-end security demands

seem to allow for all such architectures to have a role with varying scope and limitations. This further underscores the argument to provide a negotiable interface protocol.

4. CAPWAP Component Architecture

Given the preliminary outline of the three primary architecture types (and a fourth variant) in Section 3.3 the predominant architectural components are presented in three perspectives:

1. Functional & Service-based (WLAN standards)

2. Architectural Split

3. Topological

This is required as a means to realize the way the three aspects are inter-dependent.

The Figure 1 illustrates the basic outline of communications architecture between AP & AC.

```
       |                          _  |
       |    Control/Provisioning ( )-|----Security
       |<------------------------|-|>|
       |      Status/Download    (_) |
       |                             |
       |                          _  |
       |            Data         ( )-|----Security
       |<------------------------|-|>|
       |        Forwarding       (_) |
       |                             |
```

```
        |                              |
        |          Discovery           |
        |<---------------------------->|
        |                              |
        |                              |
        |                              |
     +------+                     +--------+
     |Light |                     | Access |
     |Weight|                     | Router |
     |  AP  |                     |        |
     +------+                     +--------+
```

Figure 1: Basic Communications Framework

4.1 WLAN functions and Services

The IEEE 802.11 standard [1] says very little about the functionality

required of an AP. There is some discussion of the AP at a block diagram level, in the General Description in clause 5 of the standard. There, an AP is described as containing functional blocks for 802.11 station services and for distribution system services. Station services consist of the following four services:

a) Authentication

b) Deauthentication

c) Privacy

d) MSDU Delivery

Distribution system services consist of the following five services:

a) Association

b) Disassociation

c) Distribution

d) Integration

e) Reassociation

There are additional services that are required of an AP, that are described in the MAC Layer Management Entity (MLME) in clause 11. These additional management services are

a) Beaconing

b) Synchronization

c) Power Management

Other functionality that is not described, except implicitly in the MIB, is control and management of the radio-related functions of an

AP. These include:

a) Channel Assignment

b) Transmit Power Control

c) Clear Channel Assessment

d) Radio Resource Measurement (work currently under way in IEEE 802.11k)

The 802.11h [13] amendment to the base 802.11 standard specifies the operation of a MAC management protocol to accomplish the requirements of some regulatory bodies (principally in Europe, but expanding to others) in these areas:

a) RADAR detection

b) Transmit Power Control

c) Dynamic Channel Selection

4.1.1 Access Point Functions and Services

The services that MUST be in a lightweight AP are those that are directly related to the real-time aspects of the 802.11 MAC protocol and those related to the radio nature of an 802.11 AP. These functions are:

a) Privacy

b) MSDU Delivery

c) Beaconing

d) Synchronization

e) Power Management

f) Channel Assignment

g) Transmit Power Control

h) Clear Channel Assignment

i) Radio Resource Measurement

j) RADAR detection

4.1.2 Access Controller Functions and Services

The functions that MAY be moved from the lightweight AP and located in the AR are those dealing with the management and control aspects of an 802.11 AP. These are the distribution system services, in

addition to authentication and deauthentication services. These functions are:

a) Authentication

b) Deauthentication

c) Association

d) Disassociation

e) Reassociation

f) Distribution

g) Integration

h) Dynamic Channel Selection

i) Dynamic Control of transmit power

4.1.3 Other Conventional WLAN Functions and Services

"Heavy" Access Points being the bridge to the wired world MAY (and normally do) also support various services and protocols that provide seamless connectivity of WLAN clients to the wired network such as

a) Port and Protocol-based VLANs

b) SNMP

c) QoS (DiffServ and 802.1Q) mapping

d) IP routing

e) DHCP relay/server

f) RADIUS client/proxy

g) MobileIP (client proxy)

Based on the definition of lightweight access points these services SHOULD qualify for offloading to the AR.

4.1.4 Architectural Trends

4.2 CAPWAP Network Topology

The CAPWAP network topology primarily consists of the WLAN topology and the AP-AC (AP-AR) topology.

The WLAN topology is straightforward and is as described in Overview section. This is not of much current interest as the relevant portal variants of WLAN are applicable equally to all new AP-AC topologies.

4.2.1 Functional Distribution of WLAN Services

Functional distribution of WLAN services described in earlier sub-sections are partly an artifact of the architecture types ARCH0-3. However, they may result in AP-AC topological constraints. Such constraints include direct connectivity to the AC being required and in most cases mandate L2 connectivity.

4.2.2 AP to AR Topologies

CAPWAP assumes that the AR and AP are within the same administrative domain, i.e. they are owned/controlled by the same entity. CAPWAP makes no topological assumptions beyond these, meaning there are several topologies which must be considered for our purposes.

```
      ---------------------------------------------------------------------


                           -------+------ LAN
                                  |
                          +-------+-------+
                          |  + + AR  + +  |
                         +----+-----+----+
                               |     |
                           +---+     +---+
                           |             |
                        +--+--+       +--+--+
                        | AP  |       |  AP |
                        +--+--+       +--+--+

      ---------------------------------------------------------------------
```

Figure 2: Directly Connected


```
      ---------------------------------------------------------------------


                           -------+------ LAN
                                  |
                          +-------+-------+
                          |  + + AR  + +  |
                          +----+-----+----+
                               |     |
```

```
                             +---+     +---+
                             |             |
                          +--+--+    +-----+-----+
                          | AP  |    |   Switch  |
                          +--+--+    +---+-----+-+
                                         |     |
                                      +--+--+  +----+
                                      | AP  |       |
                                      +--+--+    +--+---+
                                                 | host |
                                                 +------+

      ----------------------------------------------------------------------

                     Figure 3: Switched Connections
```



```
      ----------------------------------------------------------------------

                            +-------+-------+
                            |  + + AR  + +  |
                            +-------+-------+
                                    |
                            --------+------ LAN
                                    |
                            +-------+-------+
                            |     router    |
                            +-------+-------+
                                    |
                            -----+--+--+--- LAN
                                 |     |
                             +---+     +---+
                             |             |
                          +--+--+       +--+--+
```

```
                             |  AP  |        |  AP  |
                             +--+--+         +--+--+

          ----------------------------------------------------------------------
```

Figure 4: Routed Connections

4.3 CAPWAP Security

The CAPWAP architecture spans more than the topology over the air. IEEE 802.11 (and now 802.11i) describes the single-hop security over-the-air.

The resulting security scheme only protects the data frames (multicast, broadcast and unicast) between stations and AP.

This leaves a security gap in the CAPWAP topology between AP and AC (AR).

As discussed earlier security of control and management traffic between the AP and AR subsystem, needs to be secured, failing which control of AP can be compromised.

In addition there may be explicit requirements to secure the data flow between AP and AR segment. This is end-end traffic between WLAN stations and their WLAN/wireline destinations invariant to CAPWAP considerations. Protection of this traffic in this segment may incidentally ensue in architectures such as in ARCH2 and ACRH3.

4.3.1 WLAN Security

802.11 provides layer 2 authentication and privacy services. Severe deficiencies have been documented in the mechanisms of the original standard. The current task group, 802.11i, is completing work on an amendment to the standard that addresses these deficiencies. The requirements for 802.11i are more difficult than simply providing the desired level of protection for the information carried by 802.11 frames in new equipment. 802.11i must also provide a mechanism that can be used by equipment already deployed, to eliminate the deficiencies of the original standard to which the equipment was built.

WLAN Security offers over-the-air single-hop MAC-layer frame security for data frames between Mobile Stations and AP's. This is built on top of 802.1X-based authentication and Session and Data-encryption Key Exchanges derived thereof.

4.3.1.1 Authentication - EAP over LAN (802.1X)

802.11i specifies an extensible authentication method, based on negotiation between the AP and mobile device that occurs during the association process. After successfully negotiating the particular authentication method to be used, the mobile device is allowed to associate, but must immediately complete the negotiated authentication before any data exchange will be permitted.

The default mechanism for authentication defined by 802.11i is to piggyback on the 802.1X standard, using EAP to authenticate the mobile device or user after 802.11 association with an AP has completed. In the terms defined in 802.1X, an AP is an authenticator and a mobile device is a supplicant. The AP, as authenticator, proxies the supplicant's communications to an authentication system. An example authentication system is a RADIUS server. The AP communicates with the RADIUS server, as a RADIUS proxy for the client, using EAP. The AP is responsible for blocking the (logical) controlled port for the associated device until the successful completion of the 802.1X authentication. At the conclusion of the 802.1X authentication, keying material is available to both the mobile device and AP that can be used for frame security.

4.3.1.2 Frame Security (802.11i)

802.11i Frame Security offers Encryption, Message Integrity and Replay Protection services.

To meet the requirements of improving security for both existing devices and new devices, 802.11i specifies two security mechanisms,

the Transition Security Network (TSN) and the Robust Security Network (RSN). Both TSN and RSN utilize keying material derived from an 802.1X-based authentication exchange to deliver a pair-wise master key (PMK) to both the mobile device and AP. TSN can also use a preshared key (PSK) to derive a PMK without the use of an authentication exchange. From the PMK is derived a pair-wise transient key (PTK). The PTK is used to create a pair-wise temporal key (TK), an EAPOL key encryption key (KEK), and an EAPOL key confirmation key (KCK). An 802.1X exchange is also used to deliver the keying material to derive a group master key (GMK). From the GMK is derived a group transient key (GTK). The GTK is used to create a group temporal key (TK) used by the AP to encrypt multicast frames and by the mobile devices to decrypt multicast frames.

TSN specifies a means to improve the security of equipment built with the original RC4-based wired equivalent privacy (WEP) cipher. TSN requires that the encryption key used with WEP be rotated on every packet. TSN specifies the algorithm for this key rotation, based on the pair-wise TK and the frame sequence counter. In addition, TSN specifies an algorithm for a keyed message integrity code (MIC) (more often called message authentication code (MAC), but that acronym is already utilized in the 802.11 standard), called Michael. Michael is a compromise between strength and computational requirements, because this must operate on legacy equipment with fixed computational capabilities. As a result, TSN also specifies some rather severe countermeasures to be implemented when an attack against the MIC is suspected.

RSN specifies an encapsulation and algorithm for new equipment that is significantly stronger than either WEP or TSN. The algorithm is an AES mode called Counter Mode with CBC-MAC (CCM)[3]. This AES mode provides data privacy, data integrity, and source integrity with low additional computational requirements beyond data privacy, alone.

4.3.2 Mutual Authentication of AP and AR

As detailed in Section 4.3, the need to enforce secure communication requires a mutual strong authentication protocol and an associated Key Management protocol that derives from the trust established the authentication phase. The resulting key material is used to derive session keys and subsequent key agreement for setting up secure encapsulation of AP-AR meta-communications.

The Key Management protocol choices are governed by the worst-case specification of Lightweight AP (LAP) capabilities.

4.3.3 Path Security of AP and AR

The secure communications MUST support confidentiality, message authentication and replay protection. The choice of ciphers should consider the required strength and threat model as well as the compute capabilities, real-time nature and relative bandwidth of such traffic.

4.4 AP Provisioning

In order to create a trust model between the AP subsystem and AC subsystem for secure communications enabling automatic discovery, configuration and adaptive resource management the AP's need to be set up securely in the AC(AR)'s domain.

4.4.1 AP Identity

Identity of the AP is established reliably by cryptographically secure binding of an AP's unique identity such one of its wireline MAC addresses to a cryptographic key.

4.4.2 AP Configuration

Configuration of an AP includes providing the parameters necessary for the AP to advertise and provide service for one or more WLANs. These parameters are both physical and logical.

Physical parameters are related to the operation of the AP's radio interface. These include the channel on which the AP is to operate, the maximum power at which the AP is to transmit, antenna selections, the supported data rates, and the timing for the periodic announcements of the WLANs provisioned on the AP.

Logical parameters are related to the individual WLANs that are provisioned on the AP. These include the SSID of the WLANs, the allowed authentication methods, the allowed privacy methods, values for the contention-free period and DTIM, VLAN associations, IP addresses and netmasks, authentication server addresses, any pre-shared keys for WLANs or authentication servers, regulatory (country) information, and other 802.11-specific capabilities to be advertised for the WLANs.

4.4.3 Access Router Availability

Also discussed later in Section 4.6 in discovery context, as part of provisioning an AP one may configure the ability to offer redundancy of ACs or based on negotiated architecture. Constrained architectures with limited AP-AR topologies may be unable to offer flexible

redundancies and may require hardware supported alternatives.

4.5 Access Point Service Management

In a large WLAN system with many APs, continuous management of those APs is necessary to enable quick reaction to changes in service capabilities caused by internal or external factors such as dynamically varying hotspot loads and time-variant fluctuations in RF interferences due to extraneous negihborhood devices. An adaptive RF management based on dynamic systemic monitoring and power and frequency management is needed to be driven from ACs (or at times a hierarchy of ACs).

4.5.1 Monitoring

Each AP in a WLAN must be monitored for a number of variables. This is needed to be able to assess the ability of the individual AP to meet the service demands placed upon it. Among the variables that need to be monitored are:

a) instantaneous data load

b) peak and average load over a configurable monitoring period

c) Measurements of interference from neighboring BSS's

d) number of mobile devices associated

e) statistics for each associated mobile device

f) Signal Strength of Received Frames

g) RADAR detection

4.5.2 Control

Maintaining the operation of a large WLAN system at or near its peak capability requires that the individual APs that comprise that system must be controlled to adapt to changes in the internal or external factors that affect the performance of the system as a whole. In particular, the aspects of an AP that require control are the following:

a) Access Controller to which the AP is connected

b) enabling and disabling the operation of the AP

c) Enabling and Disabling operation of individual radios at an AP

d) establishment and update of session keys for protection of AC/AP communication

e) Radio channel for transmission

f) Transmit Power

4.6 Access Router Discovery

When a AP comes alive on a network it may authenticate and register with one or more ARs it detects on the network it is connected to. In some architectures today the ARs are the bridges they directly connect to. It performs a AR discovery procedure in its network neighborhood. Based on the Network Topology and Layering it MAY attempt a L2 or IP discovery of ACs. This will also depend partly on the architectural capabilities of the AP and of available ARs. The type of discovery protocol is also dependent on prior one-time Provisioning of AP (configuration). The identification of ARs is only dependent on the L2 or IP protocol used but is expected to be architecture-agnostic. It is the Capability Negotiation Phase (Section 4.6.2) that follows which resolves the mutual capabilities of AP and AC which lets them decide to AP register with one or more AC.

4.6.1 Access Router Availability

CAPWAP discovery entails the ability of an AP to failover to another AR in the same domain (ESS) in the event of the failure of the current AR.

Failure detection and failover may use existing IP protocols such as VRRP or extensions thereof.

4.6.2 Capabilities Negotiation

An AP performs AR discovery in its network neighborhood. Upon having discovered available ARs the AP enters into a capabilities exchange phase with the candidate ACs. If the architectural types match during the exchange - the AP registers with the AC and configures itself based on the policies it derives from the AC after mutually authenticating with the AC. The capabilities negotiated by architectural type match will decide the applicable API's between AP and AC.

4.7 Summary

The CAPWAP allows for a set of flexible architectures as described in Section 4.1.4 The architecture proposes the following set of CAPWAP services to achieve the Security, Ease of Management, Enhanced QoS and Mobility objectives across the WLAN domain:

o AC Discovery

o Capability Negotiation

o Mutual Authentication of AP and AC

o Secure Encapsulation Protocol based on Secure Key Management

o Secure AP Configuration from AC

o Secure Encapsulation of Control and/or Data between AP & AC

5. Prior Work

Related work on such problems have been dealt with in Academia (Section 5.1) and standards (Section 5.2). The former is more directly related to the proposed CAPWAP architecture. The latter is a generic solution attempted to address distributed data-forwarding front-ends with highly available control-plane backends.

5.1 DIRAC

DIRAC is a DIstributed Router ArChitecture for wireless networks, independently developed by a research group in UCLA. DIRAC [16] adopts a very similar distributed architecture to what is proposed here that is composed of a generic Router Core (RC) shared by the wireless subnets and a lightweight and network specific Router Agent (RA) at each access point/base station. The Router Core in DIRAC corresponds to AR in CAPWAP while the Router Agents are the APs.

While the architecture and end goals of DIRAC are very similar to CAPWAP, there are several difference that are worth pointing out:

o The Router Core at DIRAC is intended to be generic and agnostic to the L2 radio technology being used between the Router Agent and the client terminals. This is achieved by terminating the radio specific L2 connection at the Router Agent while the statistics/ actions(i.e.,control)/events messages that are exchanged between the Router Core and the Router Agent are abstracted into a different and generic packet format. CAPWAP, on the other hand, simply encapsulates the 802.11 management frames from APs to ARs so that ARs have to fully understand 802.11 frame format.

o No security is being considered in the DIRAC work which is probably ok for academic research but not ok for IETF standard.

o The DIRAC paper focuses less on the protocol between the RC and RA but a lot more on the architecture and implementation issues in this work. The protocol consists of three kinds of messages: statistics, actions (i.e., controls) and (asynchronous) events. DIRAC does not consider the issue of discovery and firmware image downloading etc.

o The DIRAC paper provides three prototype wireless services that are implemented within the DIRAC framework to demonstrate not only the potential performance gain but also the viability of these new wireless services being enabled by such a framework. These examples provide some nice academic data points for CAPWAP.

5.2 ForCES

The IETF ForCES (Forwarding and Control Element Separation) group was chartered to "define a framework and associated mechanisms for standardizing the exchange of information between the logically separate functionality of the control plane, including entities such as routing protocols, admission control, and signaling, and the forwarding plane, where per-packet activities such as packet forwarding, queuing, and header editing occur. By defining a set of standard mechanisms for control and forwarding separation, ForCES will enable rapid innovation in both the control and forwarding planes. A standard separation mechanism allows the control and forwarding planes to innovate in parallel while maintaining interoperability."

5.2.1 Similarities in Objectives and Architectural Considerations

While ForCES aims to provide interoperability between CEs and FEs from different vendors, CAPWAP has a very similar goal in mind -- to allow APs and ARs from different vendors interoperable when mixed and matched in the wireless access networks. Even though ForCES originally was heavily focused on routers to achieve interoperability between Forwarding Elements (FEs) and Control Elements (CEs) inside a router (i.e., Network Element -- NE), many similarities or analogies can be found between ForCES architecture and CAPWAP architecture:

o "The APs can be considered as remote RF interfaces, being controlled by the AR" [LWAPP spec] -- it is clear that APs in the CAPWAP architecture can be viewed as FEs in the ForCES architecture, or more precisely, APs can be viewed as a specific wireless port function (Logical Functional Block, LFB, using ForCES's terminology) that is part of the FEs.

o The LWAPP-related functionality of AR in the wireless access network is mostly control plane related and hence the AR can be considered a CE from the ForCES point of view. It should be noted that the AR also performs forwarding functions, and as such, could also be internally viewed as a CE/FE combination, although usage of ForCES to control APs by the AR would not necessitate usage of ForCES within the AR.

o "AR + multiple lite-weight APs" as a whole then can be considered as a distributed router with some parts of the FEs (APs) physically separated from the CEs.

5.2.2 Overlap in Topology Considerations

While it is possible to construct a NE out of CEs and FEs which are physically separated by a routed (L3) cloud, ForCES constraint itself to focus on very close localities consisting of CE and FEs that are either components in the same physical box, or are separated at most by one local network (L3) hop. This topology overlaps with the three topologies -- directly connected, switched (L2), or routed (L3) -- considered by CAPWAP as well. But if CAPWAP support arbitrary routed cloud (with multiple L3 hops) between AP and AR, we need to carefully examine ForCES and see if it can accommodate such topology while still satisfying all the requirements including security.

5.2.3 Differences in Design Approach

The general design behind ForCES is to separate the base protocol from the actual information elements that carry the control/configuration/monitoring/events messages between the CE and FE, due to the diversity of FE functions among data plane vendors. The information elements that are specific to any particular FE (e.g., IPv4 forwarding, or DiffServ, or MPLS) are represented in FE model. Such design allows ForCES to be very flexible and extensible to accommodate wide spectrum of data plane functions, possibly including IEEE 802.11 wireless AP functions. The current LWAPP protocol is taking a very different design approach. LWAPP is a very domain specific protocol. While the general domain for LWAPP can potentially include any wireless radio technologies, the current spec of LWAPP is very much IEEE 802.11 specific and many of the 802.11 functions are assumed and built into the protocol directly.

5.2.4 Differences in the Functionality Controlled

The FE functions being controlled by CE via ForCES are mostly L3 and L4, but sometimes L2 (e.g., ARP). On the other hand, the AP functions that are being controlled by ARs are mostly L2 (IEEE 802.11MAC), but sometimes higher layer as well (if those functions reside on APs).

5.2.5 Similarties in Security Requirements

The security requirements in both the CAPWAP and ForCES appear to overlap significantly, in terms of secure association, authentication, confidentiality, integrity, anti-replay, etc. Even though ForCES has not finalized on its protocol selection (among three proposals) yet, ForCES framework document recommends that ForCES adopt one of the standard security mechanisms (IPsec or TLS). More close examination of security requirements and mechanisms employed in ForCES and CAPWAP is needed here.

5.2.6 Difference in Operation Scope

Even though no specific discovery mechanism is specified in the current LWAPP spec, CAPWAP does consider AR discovery in scope; on the other hand, ForCES considers the process of CE and FE discovering each other out of scope. ForCES assumes CEs and FEs enter the post-association phase with knowledge of which corresponding entities they are authorized to communicate with, but ForCES itself does not address how pre-association is done.

5.2.7 Comparision in Protocols

ForCES currently has three protocol proposals and the WG has just started the protocol evaluation and selection process. Therefore, it is difficult to compare LWAPP with ForCES at the moment from the protocol view-point, unless one compares LWAPP with all the three proposals first.

But ForCES requirement document captures all the important requirements that ForCES protocol is supposed to support. Merely comparing LWAPP with this set of requirements can already provide some insight.

The most obvious difference in the two protocols may very well be due to fundamentally different design philosophies behind the two as pointed out in Section 5.2.4. LWAPP is a domain specific protocol withsome messages assuming 802.11 sematics, while the base ForCES protocol only supports the general procedures involved for setting up association between the CE and FE, CE querying FE its capability and configuration state (if any), CE provisioning FE according to the basic capability leaned in the querying stage, and FE reporting statistics and asynchronous events to CE, etc. In the context of ForCES, the messages with 802.11 specific semantics would not appear in the base ForCES protocol. Instead, an 802.11 FE (or LFB) model would have to be specified to support all the 802.11 specific configuration, statistics, and events.

Another major difference is on reliability requirement. The ForCES protocol is required to support strict reliability for mission critical payloads. On the other hand, LWAPP does not assume any reliability between the AR and AP, because it is built on top of L2 or IP directly.

One thing that LWAPP supports but none of the ForCES protocol proposals directly address is firmware image downloading.

6. Security Considerations

One of the major goals of the CAPWAP architecture is to ensure strong authentication of AP to the registered AR and secure communications between them as described in the preceding sections.

AR-AP traffic can be classified into: data traffic (e.g. from or to an end user), and control traffic which is strictly between the AR and AP. Since data traffic may be secured end-to-end security mechanisms outside the scope of this work, we confine our solution to control traffic. The resulting security consists of two components: an authenticated key exchange, and control traffic security encapsulation. The security encapsulation may be accomplished using relatively lightweight mechanisms such as CCM, described in [2]. This encapsulation provides for strong AES-based message authentication and encryption. Detailed discussions of such possible security protocol alternatives is out of scope in this document.

7. Acknowledgements

The authors wish to thank the timely inputs and discussions provided by Pat Calhoun towards completion of this document in a very short time. In no less measure our thanks go to Scott Kelly et al in kindly consenting to let us adapt from their topological and architectural analysis in [5] that helped us shorten the time to draft. The authors also wish to thank IESG & IAB for their feedback, particularly Randy Bush, James Kempf and Bernard Aboba for the discussions that has helped focus this draft objective. Thanks are also due to Dorothy Stanley in this regard for the IEEE perspective.

References

[1] "IEEE WLAN MAC and PHY Layer Specifications", August 1999, <IEEE 802.11-99>.

[2] "Advanced Encryption Standard (AES)", November 2001, <FIPS PUB 197>.

[3] "Counter with CBC-MAC (CCM)", September 2003, <RFC 3610>.

[4] "Light Weight Access Point Protocol (LWAPP)", June 2003, <http://www.ietf.org/internet-drafts/draft-calhoun-seamoby-lwapp-03.txt>.

[5] "Security Requirements for a Light Weight Access Point Protocol", August 2003, <http://www.ietf.org/internet-drafts/draft-kelly-ietf-lwapp-sec-00.txt>.

[6] "The Internet Standards Process Revision 3", October 1996, <ftp://ftp.isi.edu/in-notes/rfc2026>.

[7] "Key words for use in RFCs to Indicate Requirement Levels", March 1997, <ftp://ftp.isi.edu/in-notes/rfc2119>.

[8] "Mobility Related Terminology", April 2003, <ftp://ftp.isi.edu/internet-drafts/draft-ietf-seamoby-terminology-04.txt>.

[9] "Extensible Authentication Protocol (EAP)", September 2003, <http://www.ietf.org/internet-drafts/draft-ietf-eap-rfc2284bis-06.txt>.

[10] "WiFi Protected Access (WPA) ver 2.0", April 2003.

[11] "IEEE Std 802.11i/6.0: Specification for Enhanced Security", September 2003.

[12] "IEEE Std 802.11F: Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol across Distribution Systems Support 802.11 Operation", July 2003.

[13] "IEEE Std 802.11h: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe", October 2003.

[14] "IEEE Std 802.1X: Port-based Network Access Control", June 2001.

[15] "IEEE Std 802.1Q: Virtual Bridged Local Area Networks", May

2003.

[16] "DIRAC: A Software-based Wireless Router System", 2003.

Authors' Addresses

Mahalingam Mani
Avaya Inc.
1001 Murphy Ranch Rd
Milpitas, CA 95035

Phone: +1 408-321-4840
EMail: mmani@avaya.com

Bob O'Hara
Airespace
110 Nortech Parkway
San Jose, CA 95134

Phone: +1 408-635-2025
EMail: bob@airespace.com

L. Lily Yang
Intel Corp.
MS JF3 206, 2111 NE 25th Avenue
Hillsboro, OR 97124

Phone: +1 503-264-8813
EMail: lily.l.yang@intel.com

Intellectual Property Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.